Before the
Federal Communications Commission
Washington, D.C. 20554

In the Matter of	)	
	)	
Communications Assistance for Law	)	ET Docket No. 04-295
Enforcement Act and Broadband Access	)	
Services	)	RM-10865
	)	

VeriSign, Inc. Opposition

Request for Stay Pending Issuance of Subsequent Orders and for Stay Pending Judicial Review

Center for Democracy and Technology, et al.

Anthony M. Rutkowski
Vice President for Regulatory Affairs
VeriSign Communications Services Div.
21355 Ridgetop Circle
Dulles VA 20166-6503
tel: +1 703.948.4305
mailto:trutkowski@verisign.com

Peter Wiederspan
Director, NetDiscovery Service
4501 Intelco Loop SE
Olympia, WA 98503
Tel: +1 360.493.6220
mailto: pwiederspan@verisign.com

Michael Aisenberg
Director, Government Relations
1666 K Street, N.W., Suite 410
Washington DC 20006-1227
Tel: +1 202.973.6611
mailto:maisenberg@verisign.com

Brian Cute
Director, Government Relations
1666 K Street, N.W., Suite 410
Washington DC 20006-1227
tel: +1 202.973.6615
mailto:bcute@verisign.com

Filed: 2 December 2005

1. On 5 August 2005, the Commission adopted its *First Order* in this proceeding.[1] On 23 November, the Center for Democracy & Technology, American Library Association, Association for Community Networking, Association of College and Research Libraries, Association of Research Libraries, Champaign Urbana Community Wireless Network, Electronic Frontier Foundation, Electronic Privacy Information Center, Pulver.Com, Sun Microsystems and Texas Internet Service Providers Association (Petitioners) filed with the Commission a *Request for Stay Pending Issuance of Subsequent Orders and for Stay Pending Judicial Review (CDT Request)*. VeriSign, Inc. (VeriSign) is an interested party in this proceeding and hereby submits this opposition to the *CDT Request* pursuant to Sec. 1.45(d) of the Commission's rules.

2. Petitioners in the *CDT Request* seek "…both a stay of the Commission's First Report & Order pending the release by the Commission of the subsequent orders anticipated by that first Order, and a stay of the First Report & Order pending review of that Order by the U.S. Court of Appeals for the District of Columbia Circuit."[2] The *CDT Request* should be denied for the following compelling considerations.

I. THE CALEA *FIRST ORDER* WAS CAREFULLY DEVELOPED AND NARROWLY TAILORED TO RESPOND TO AN URGENT NEED FOR DEFINITIVE, REASONABLE NETWORK FORENSIC CAPABILITIES UNIQUELY AVAILABLE FROM SPECIFIC ACCESS AND VoIP PROVIDERS

3. The activity surrounding this proceeding began more than five years ago when the Internet Protocol (IP) started to be used significantly as a replacement protocol within the nation's public telecommunication network infrastructure, followed by the emergence of IP-based emulations of public network call signalling protocols and their introduction as commercial public services. As this technical and operational evolution began to unfold, the U.S. Department of Justice (USDOJ) and their counterparts worldwide began working closely with industry to assure needed forensic capabilities to assist law

---

1 *See First Report and Order and Further Notice of Proposed Rulemaking* in the Matter of Communications Assistance for Law Enforcement Act and Broadband and Access Services in ET Docket No. 04-295, RM-10865, Doc. FCC 05-153, 20 FCC Rcd 14989 (23 Sept 2005) ("First Order").

2 *CDT Request* at iii.

enforcement remained available – successfully progressing the work in multiple domestic and international workshops, conferences, requirements documents, and standards bodies. Especially noteworthy were two major workshops in 2003 - sponsored by the FBI to discuss the requirements with industry and make available two detailed requirements documents. Finally, in early 2004 after extensive industry collaboration to achieve the development of these capabilities, the USDOJ, FBI, and DEA jointly took steps to initiate the instant proceeding – aimed at providing a minimal, consistent, ubiquitous forensic "handover" capability in the public network infrastructure that was available to acquire evidence when authorized pursuant to law.

4. After 18 months and two commenting cycles in the instant proceeding that included more than 700 comments, the Commission's *First Order* was adopted - taking narrow and carefully determined steps to institute CALEA-based forensic capabilities that were not only developed within the industry together with law enforcement, but also started to become deployed in anticipation of the Commission's actions in this proceeding. Substantial investments have been made within the industry generally, and by VeriSign in particular, to achieve this compliance capacity for providers.

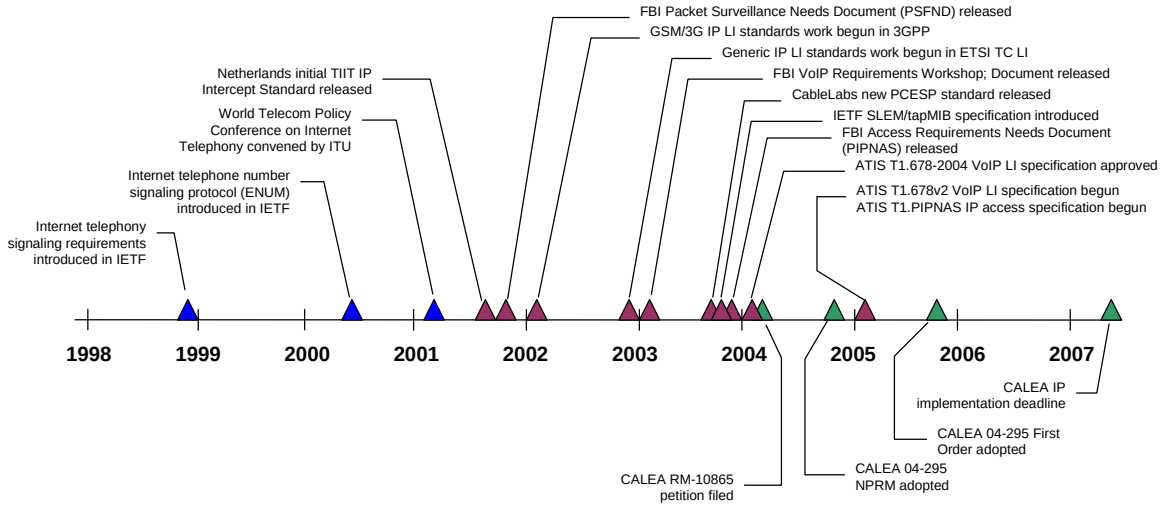

Fig. 1. IP-Enabled Public Communications Infrastructure - CALEA Continuum Timeline

5. Petitioner's arguments of arbitrariness and capriciousness are not supportable in light of the facts. Figure 1, above, provides a general overview of the instant proceeding (green triangles) against the backdrop of infrastructure evolution (blue

triangles) and industry - law enforcement collaborative activities (plum triangles). This extensive cooperation and consultation has ensued pursuant to Secs. 103, 104, 106 and 107 of the CALEA statutory provisions, exactly as Congress intended.[3] It has involved the work of hundreds of individuals and scores of companies working together over the past several years in more than a dozen different domestic and international industry standards forums to produce the necessary capabilities specifications required in the Commission's *First Order*. This collaboration in turn has resulted in the communications and network forensics industries investing significantly in the development and deployment of equipment, software, and facilities in anticipation of Commission's *First Order*. The requirements for full compliance with the *First Order* have been known for nearly three years, and the means of complying at low-cost with no adverse effects on technology are available today. Affected service providers have two readily available options: implement the requirements themselves or through available service bureaus.

A. The Commission's 18 Month Deadline Seems Well Considered and Compatible with Continuing Industry Developments

6. The Commission's 18 month deadline for a digital forensics law enforcement support capability - imposed pursuant to either CALEA or Title I authority on facilities-based broadband Internet access providers and PSTN interconnected VoIP providers nearly 8 years after the technology first began to be standardized for introduction as part of the national public telecommunication infrastructure, four years after the release of the FCC's detailed requirements document, three years after commercial solutions appeared in the marketplace, and at a point where use of the technology is in U.S. households is projected to grow from 400,000 in 2004 to 12.1 million in 2009 - is neither arbitrary nor capricious.[4] The deadline seems well considered and highly appropriate in light of these trends. Indeed, exercising Title I authority, the Commission has adopted public safety

---

[3] *See Communications Assistance for Law Enforcement Act of 1994*, Pub. L. No. 103-414, 108 Stat. 4279.

[4] *See Broadband Telephony: Leveraging Voice Over IP to Facilitate Competitive Voice Services*, Jupiter Research, Oct 2004. *See also*, Cybertelecom, VoIP Statistics <http://www.cybertelecom.org/data/voip.htm>

E911 capability requirements within much shorter timeframes.[5] Whether the capability requirements are for public safety, forensic support for law enforcement, infrastructure protection, consumer protection, or national security/emergency preparedness, such actions are consistent with the Commission's authority accorded by Congress and affirmed by the Court.[6]

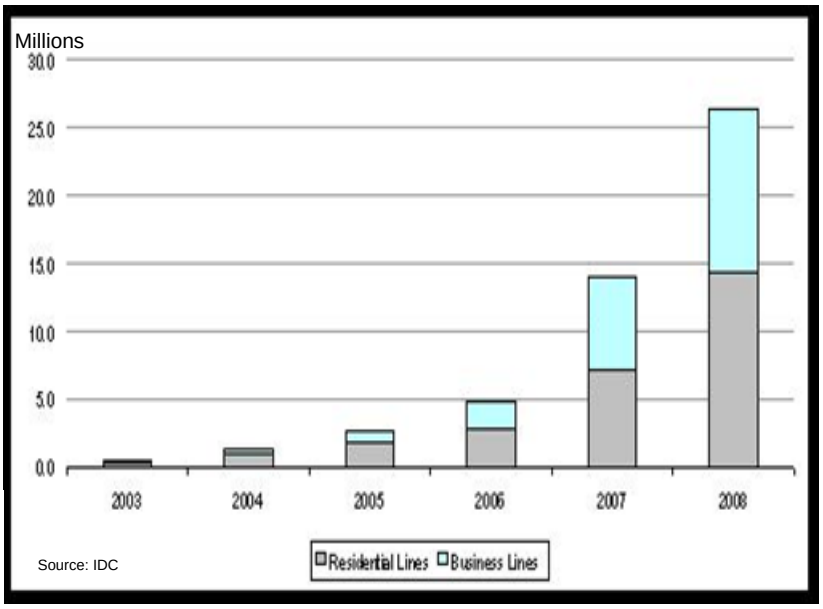

Fig. 2. Increase in North American VoIP Telephone Lines

7. In light of the rapid transition of the public telecommunication infrastructure to IP-enabled systems and VoIP now underway, it would be especially inappropriate for the Commission to delay implementing the *First Order* CALEA requirements. See Fig. 2, above. At this point in the ongoing technological transition, it is relatively easy and inexpensive for vendors to include the required network forensic features in the new systems being built, and for service providers to implement the capabilities to meet CALEA mandates. The ensuing 18-month period is precisely when it makes good public policy sense to uniformly implement the capabilities. Furthermore, the mandated capabilities are generic, and not technology dependent. Delaying implementation of the

---

5 *See First Report and Order and Notice of Proposed Rulemaking*, In the Matters of IP-Enabled Services (WC Docket No. 04-36) and E911 Requirements for IP-Enabled Service Providers (WC Docket No. 05-196), Doc. FCC 05-116, 3 June 2005.

6 *See id*. at para. 4; *National Cable & Telecomms. Ass'n* v. *Brand X Internet Servs.*, 125 S. Ct. 2688 (2005) (hereinafter referred to as *Brand-X*).

CALEA capabilities would potentially result in more costly retrofitting of systems to become compliant at a later date.

B. The Compliance Measures for VoIP and Internet Broadband Access Have Long Been Well Known

8. Petitioner's arguments for resetting the 18-month clock are based on assertions that the "…FBI/DOJ have failed to inform the Commission or the public what they believe CALEA compliance means in the Internet context" – with citations to impromptu remarks by Bureau officials.[7] In fact, the Federal Bureau of Investigation (Bureau) initially made the requirements known more than four years ago.[8] The precise capabilities at issue here were explicitly conveyed to industry in 2003, and the Bureau conducted two day-long industry workshops at the time of the requirements release to help clarify these specifications and allow interaction with a broad array of industry attendees.[9] Several other widely attended industry workshops and other outreach initiatives were conducted by the Bureau's CALEA Implementation Section and Quantico Engineering Research Facility. The capability specifications were also provided upon request via the well-known CALEA Implementation Section website.[10] Over the subsequent years, scores of meetings and thousands of hours of productive work have ensued in domestic and international industry standards forums with active involvement of the Bureau and their contractors and virtually every sector of the telecommunications and network forensics industry. As a result, multiple standards have been produced to meet the capability requirements – which in turn have resulted in equipment being produced, capabilities tested, and services offered.[11]

---

7 *CDT Petition* at 15.

8 *See Packet Surveillance Fundamental Needs Document (PSFND) for Telecommunications Carriers, Equipment Manufacturers, and Providers of Telecommunications Support Services*, Issue 1.0, October 31, 2001, CALEA Implementation Section, Federal Bureau of Investigation.

9 *See, e.g., Electronic Surveillance Needs for Carrier-Grade Voice over Packet (CGVoP) Service*, Issue 1, January 29, 2003, CALEA Implementation Section, Federal Bureau of Investigation; Surveillance for Voice over Packet Summit, 23 Jan 2003 at Chicago; *Electronic Surveillance Needs for Public IP Network Access Service (PIPNAS)*, Issue 1, September 30, 2003, CALEA Implementation Section, Federal Bureau of Investigation; LAES for Public IP Network Access Service (PIPNAS) Summit, 2 Oct 2003 at Chicago.

10 *See* www.askcalea.com, www.askcalea.net, www.askcalea.org.

11 *See, e.g., PacketCable™ Electronic Surveillance Specification*, PKT-SP-ESP-I04-040723; Cable Labs, 23 Jul 2004; *Lawfully Authorized Electronic Surveillance (LAES) for Voice over Packet Technologies*

E. The Issue of Who Is Covered Is Severable from Compliance

9. In almost any significant rulemaking proceeding requiring new or additional infrastructure capabilities involving many diverse providers, the Commission and industry together are always faced with implementation uncertainties that go to questions of timing. Inevitably a general rule must be established, and the Commission is faced with variables involving specific technologies, classes of providers, and the situations of individual providers. Promulgation of the general rule is severable from the specific circumstances of network service providers under the *First Order*.

1. The Commission should continue to consider the scope of the private network exemption in today's IP-enabled national infrastructure

10. CALEA's private network exemption was crafted at a time when simple, well-defined compartmentalization existed between private telephony PBXs and data networks and their public telecommunication network counterparts. Today's complex public IP-enabled access network and VoIP infrastructure gets substantially blurred at the periphery with the existence of countless, nominally private "edge" networks and gateways. The boundary around "publicly available infrastructure and services" – which has constituted the traditional boundary for imposing public interest capability obligations such as CALEA, E911, NS/EP, disability assistance, etc – becomes significantly more difficult to fashion. Some extremely large "extranets" with uncontrolled access control can effectively constitute public network infrastructure. The issues and tradeoffs are complicated and deserve full treatment in subsequent phases of the instant CALEA proceeding. However, such further treatment should not be the basis for a universal stay of the *First Order* requirements.

---

in Wireline Telecommunications Networks, American National Standard for Telecommunications T1.678-2004; Draft, *Proposed for Lawfully Authorized Electronic Surveillance (LAES) for Voice over Packet Technologies in Wireline Telecommunications Networks, Version 2*, ATIS-1000678.200X; *Lawfully Authorized Electronic Surveillance (LAES) for IP Network Access*, ANS T1.IPNA-YEAR, Oct 2005; *Technical Specification, Universal Mobile Telecommunications System (UMTS), 3G security, Handover interface for Lawful Interception (LI)*, ETSI TS 133108 V6.9.0 (2005-06-27).

2. The Commission does not need to define the procedural details of exemptions, extensions, alternative implementations, or special funding for some providers prior to imposing the requirements

11. Here also, virtually all significant proceedings dealing with infrastructure requirements inevitably involve mechanisms whereby some affected providers can seek exemptions, extensions, and alternative implementations, as well as seek special funding. In the case of CALEA, all these factors are included in the CALEA statutory provisions, and deserve substantial treatment in subsequent phases of the proceeding. However, this does not mean that implementation must stand still until the matters are resolved. Such a phased approach was also adopted in the first CALEA proceeding.[12]

II. MOVANTS ARE UNLIKELY TO SUCCEED ON THE UNDERLYING MERITS OF THEIR APPEAL

A. The CALEA Statute Appears to Encompasses the Services and Providers Delineated in the Order, and Plainly Provides the Commission with Determinative Authority to So Find - in Addition to General Authority Pursuant to Title I of the Communications Act

12. Petitioners' reading of CALEA creates an "information services contamination theory" that essentially would remove authority over the entire telecommunications infrastructure today from CALEA-related Commission purview. The narrow "information services" exclusion in the CALEA Statute is asserted to equate with "the Internet" which is equated with all IP-enabled services and applications, which are then excluded from CALEA.[13] The result has the information services exception swallowing the entire telecommunications infrastructure today, leaving law enforcement with no forensic capabilities except those that they can somehow manage to implement themselves by hurriedly visiting the premises of potentially widely dispersed IP service providers and installing equipment during an investigation. In a world of highly nomadic IP network users and providers, the result would essentially eliminate the possibility of

---

[12] *See Report and Order* in the Matter of Communications Assistance for Law Enforcement Act, CC Docket No. 97-213, Document FCC 99-11, March 15, 1999; *Second Report and Order*, CC Docket No. 97-213, Document FCC 99-229, August 31, 1999; *Third Report and Order*, CC Docket No. 97-213, Document FCC 99-230, August 31, 1999.

[13] *See Joint Comments of Industry and Public Interest*, filed Nov. 8, 2004; *Joint Reply Comments of Industry and Public Interest*, filed Dec. 21, 2004. *Cf.*, Sec. 102(6), *Communications Assistance for Law Enforcement Act of 1994, supra.*

law enforcement from gathering real-time forensic evidence. The result nullifies the basic purpose of CALEA.

13. Congress intended CALEA to effect a continuing process – where, as the network infrastructure evolved, industry and law enforcement would work together to evolve the associated network forensic capability requirements under the aegis of the Commission. Petitioners conversely argue for a static CALEA – frozen in a world of communications that existed in 1994 when the Internet was still managed as a closed research network by the National Science Foundation.

14. The *First Order* requirements are drawn from an enormous base of facts together with analysis and findings. Conforming fully with *Chevron*, a determination was made that specified providers are offering services as a replacement for local telephone exchange service and it is in the public interest to make them subject to CALEA law enforcement support requirements. In addition to Commission's CALEA jurisdiction and authority, the forensic requirements mandated in the *First Order* both for law enforcement assistance and infrastructure protection would likely also pass muster under Title I authority.

B. The Commission's Construction and Application of the "Substantial Replacement Provision" Is Fully Consonant with the CALEA Statutory Language

15. Petitioners argue that the Commission has not developed a sufficient record to meet the associated substantial replacement or public interest tests found in CALEA statutory provision Sec. 102(8)(B)(ii) which gives the FCC authority to extend CALEA requirements to any "…person or entity engaged in providing wire or electronic communication switching or transmission service. The argument of insufficiency is asserted notwithstanding a substantial analysis of the facts in the *First Order* extending over six pages and the copious comment in the proceeding and public domain supporting the Commission determination. It is highly doubtful that an appellate court will reverse the Commission's order, as its construction of the CALEA statutory provisions fall well within the *Chevron* test articulated by the Court in *Brand-X*.[14]

[14] *See Brand-X* at 8-14.

III. THE EQUITIES STRONGLY DISFAVOR A STAY

A. All imposed capabilities are beneficial and largely reversible

16. Petitioners argue that somehow, a provider that implements CALEA network forensic requirements will be harmed by being "unnecessarily" compelled to implement them pursuant to the *First Order*. What the argument ignores, however, is that the capabilities are still valuable to law enforcement and for infrastructure protection. IP service providers frequently implement substantially similar capabilities for network management purposes. There is no real harm occurring. Indeed, the incurred costs are predominantly in the mediation equipment and security office – both of which can be readily outsourced with a CALEA service bureau as part of a compliance agreement. If the compliance subsequently proves unnecessary because of subsequent Commission action, the compliance arrangement can be readily terminated.

B. Some Parties Will Be Harmed if a Stay Is Issued

17. As the Commission noted in its *First Order*, VeriSign provides the mandated CALEA capability requirements today to commercial providers as a service bureau offering.[15] Both VeriSign and its customers have relied in good faith on the Commission's timely imposition of necessary digital forensic capabilities under CALEA. VeriSign has made significant investments to provide the required support capabilities to its customers. It is one of many vendors of products and services that have invested significant resources in developing the capabilities being sought by law enforcement and mandated by the Commission. Petitioners' assertion that no party will be harmed ignores the adverse effects on the many parties who developed these capabilities to meet the Commission's implementation deadline.

C. Needed Forensic Evidence Will Not be Available, and the Public Interest Will be Harmed by a Stay

18. Lastly, and most importantly, a delay in the implementation deadline beyond the 18 months already established, denies law enforcement these capabilities and impedes protection of the nation's public infrastructure. The required capabilities are critical not

---

[15] *See First Report* at n.126.

only to the investigation and prosecution of extrinsic crimes committed via communication networks, but also to detect and pursue those bent on committing criminal acts harmful to the infrastructure itself. The requirements here are appropriate not only under CALEA authority, but also Title I responsibilities for protecting the nation's communication infrastructure.

IV. THE *CDT REQUEST* SHOULD BE DENIED

19. The highly successful industry-government collaboration that has existed to implement the *First Order* capabilities should not be halted. The *CDT Request* should be denied.